Counter-Terrorism Data Mining: legal analysis and best practices

Moeckli, Daniel ; Thurman, James

FP7-SECT-2007-217862

DETECTER
Detection Technologies, Terrorism, Ethics and Human Rights

Collaborative Project

Counter-Terrorism Data Mining: Legal Analysis and Best Practices
D08.3

Due date of deliverable: 30/07/2011
Actual submission date: 30/09/2011

Start date of project: 1.12.2008 Duration: 36 months

Work Package number and lead: WP06 Dr. Daniel Moeckli
Author(s): Dr. Daniel Moeckli, University of Zurich; James Thurman, University of Zurich

Project co-funded by the European Commission within the Seventh Framework Programme		
Dissemination Level		
PU	Public	**x**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Counter-Terrorism Data Mining: Legal Analysis and Best Practices

Table of Contents

Who Should Read This Paper? Parties that may find this paper of interest include government agencies considering the deployment of data mining technologies in the counter-terrorism context, policy makers in the field of national security, counter-terrorism and law enforcement agencies, bodies that oversee intelligence or national security activities, and non-governmental organizations focussed on the field of human rights or national security.

Executive Summary

1. Counter-terrorism data mining raises concerns with regard to the right to privacy, data protection principles and the right to non-discrimination. In addition, actions based on the results of data mining operations may result in "second-order" human rights infringements.
2. Even where states provide explicit legal authorization for data mining to combat terrorism, broad scale programmes are unlikely to conform to the principle of proportionality due to the resulting interference with the right to respect for private life of a large number of innocent individuals. Additionally, programmes that prove to be of limited effectiveness or are unable to demonstrate their effectiveness cannot constitute a necessary means of protecting national security.

3. Counter-terrorism data mining may involve a violation of a number of data protection principles. Although exclusion and derogation clauses with respect to the fields of national security and criminal law enforcement are common features of data protection instruments, Article 8 of the Charter of Fundamental Rights of the European Union as well as large portions of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data always apply. Additionally, the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data call for any exceptions to its principles to be "as few as possible" and made known to the public. Finally, the European Court of Human Rights has made frequent reference to data protection principles and the Convention on Automatic Processing in its jurisprudence on the right to respect for private life guaranteed by Article 8 of the ECHR, thus treating these principles as an inherent part of the right to respect for private life.
4. Data mining programmes that are based exclusively or to a decisive extent on one or more of the grounds that are treated as inherently suspect (such as race, ethnicity, religion or sex) may never be compatible with the right to non-discrimination guaranteed by international human rights law. Data mining programmes that involve differential treatment based on other grounds may be justified if they are carried out in pursuit of a legitimate aim and in a manner that is proportionate to that aim.

1. Introduction

This is the third and final report under Work Package 6 of the DETECTER project. Here, we address the most pertinent legal issues for data mining in the counter-terrorism context. These fall within the areas of privacy or respect for private life, data protection, and non-discrimination. It is worth noting, however, that in addition to first-order violations that implicate these rights, second-order violations may occur through the use of the results of data mining. For instance, as a result of a data mining initiative, an individual could be arrested as a potential terrorist and be denied guarantees of due process or even be subject to inhuman treatment.[1] We do not address such second-order violations here. We conclude this report with a set of best practices and guidelines for providing human rights compatibility in connection with the use of data mining in counter-terrorism.

2. Privacy

2.1. Law

There are a number of legal instruments of relevance to European countries that provide for the protection of privacy. Within the framework of the United Nations, there is the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). Of relevance for European countries is the Council of Europe's

[1] See, for an extreme example, the case of Maher Arar. His designation as a terrorist led to numerous violations of national and international law. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, "Report of the Events Relating to Maher Arar: Factual Background, Vol. I" (September 2006). See also the discussion in D8.2, pp. 31-32, explaining how poor or misguided data and information collection practices can lead to unwarranted impacts on human rights, including that individuals may have "their travels and interactions with law enforcement . . . tracked." Office of the Inspector General, U.S. Department of Justice, "A Review of the FBI's Investigations of Certain Domestic Advocacy Groups" (September 2010) at 188.

Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and, within the European Union, the Charter of Fundamental Rights.[2]

2.1.1. Scope

2.1.1.1. UN Framework

Both Article 12 of the UDHR and Article 17 of the ICCPR prohibit "arbitrary interference" with any person's "privacy, family, home or correspondence", whereas the ICCPR also prohibits "unlawful interference". Similarly, the UDHR prohibits attacks upon personal honour and reputation and the ICCPR prohibits "unlawful" attacks. Additionally, both instruments impose upon states parties a positive obligation to provide legal protections against arbitrary or unlawful interference with privacy or unlawful attacks on reputation or honour.[3]

The term "privacy" is not defined in the ICCPR nor in General Comment 16, which was drafted as an elaborative supplement to Article 17 by the UN Human Rights Committee (HRC).[4] However, the General Comment does contain clarifications of the terms "arbitrary interference", "unlawful", "family", and "home". Notably, it defines "home" as the "place where a person resides *or carries out his usual occupation*."[5] Thus, the General Comment suggests that Article 17 applies to an individual's workplace and work-related life in addition to the non-vocational sphere with which the term "private" has more traditionally been associated. "Correspondence" within the meaning of the ICCPR includes telecommunications according to the General Comment.[6] The General Comment also adds that "searches of a person's home should be restricted to a search for necessary evidence and should not be allowed to amount to harassment."[7]

Of significance for the subject of data mining is the inclusion of commentary on the storage of personal data within databanks in paragraph 10 of the General Comment. This paragraph states that the gathering and storage of personal data "must" be regulated by law. It also calls on states to implement "effective measures" to protect such data from unauthorized access or use in a manner contrary to the ICCPR. Persons within states parties should also be enabled to ascertain which authorities collect or retain their personal information, and be provided with the right to have that information corrected or deleted in the event that it is false.

In terms of the application of the ICCPR by the HRC, although there have not been any complaints concerning data mining, the case of *Rojas García v. Columbia*,[8] may shed some light on what implications the Covenant might have for state utilization of data mining in the counter-terrorism context as well as consequences that may flow from the use of data

[2] As a result of the Lisbon Treaty, the Charter has become "hard law" for the European Union, opening up the possibility that claims under the Charter may be brought, with the European Court of Justice as the court of last resort for such claims.
[3] Art. 12, second sentence UDHR; Art. 17(2) ICCPR.
[4] S. Joseph, J. Schultz and M. Castan, *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary*, 2nd edn. (New York: Oxford Univ. Press, 2004), p. 477.
[5] UN Human Rights Committee, "General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17)" (1988) at para. 5 (emphasis added).
[6] Ibid., para. 8.
[7] Ibid., para. 8.
[8] (687/96).

mining. *Rojas García* dealt with the physical search of a family's home done by police in quick-raid fashion. The police, however, raided the wrong house. The HRC found that the raid constituted an impermissible interference with the claimant's Art. 17 rights since "the State party's arguments fail[ed] to justify the conduct described."[9] Joseph, Schultz, and Castan note that it is unclear whether the decision indicates that all mistaken searches would constitute a breach of Article 17 rights.[10] If the state party can present evidence that explains how the mistake occurred, it may suffice to show that the mistaken search was not arbitrary.[11]

Apart from complaints, the HRC has commented in the context of the review of state reports on the implications of the Covenant for surveillance powers of state authorities. These comments indicate that a state's legal system should provide safeguards against the use of such powers and be subject to independent oversight, with particular preference for judicial review.[12] The Committee has also expressed concern when surveillance powers are vested in certain parties who may be in a position to abuse such power. For instance, it was troubled that prosecutors could order surveillance in the case of Poland[13] and that the Postmaster-General was empowered to open and examine items in the mail in Zimbabwe.[14] With implicit reference to paragraph 10 of General Comment 16, the HRC expressed concern that the legal system of the Republic of Korea did not provide "adequate remedies" for the correction of information in databases nor for instances of abuse or misuse of such databases.[15]

2.1.1.2. European Framework

The ECHR provides a privacy-related right in the form of Article 8. Article 8(1) declares that "[e]veryone has the right to respect for his private and family life, his home and his correspondence." In addition, the Charter of Fundamental Rights of the European Union calls for the respect of privacy in its Article 7. That provision states that "[e]veryone has the right to respect for his or her private and family life, home and communications."

In contrast to the HRC, there is a relatively rich body of jurisprudence concerning the right to privacy from the European Court of Human Rights (ECtHR) and its predecessor, the European Commission of Human Rights. The ECtHR has stated that "private life" within the meaning of Article 8 represents a broad concept "not susceptible to exhaustive definition."[16] Cases involving subjects such as name, gender, sexual orientation and sexual life, identity, personal development, and the establishment and development of personal relationships have been recognized under Article 8.[17] As with the ICCPR, the ECtHR has also recognized the inclusion of business or professional activities within the remit of Article 8.[18] The Court has stated that there is "a zone of interaction of a person with others, even in a public

[9] Para. 10.3.
[10] Joseph, Schultz and Castan, supra note 3, p. 493.
[11] Ibid., pp. 493, para. 16.28
[12] See Concluding Observations on Lesotho, (1999) UN doc. CCPR/C/79/Add. 106, para. 24; Concluding Observations on Poland, (1999) UN doc. CCPR/C/79/Add. 110, para. 22; Concluding Observations on Zimbabwe, (1998) UN doc. CCPR/C/79/Add. 89, para. 25.
[13] Concluding Observations on Poland, supra note 12, para. 22.
[14] Concluding Observations on Zimbabwe, supra note 12, para. 25.
[15] Para. 17.
[16] P.G. & J.H. v. the United Kingdom, App. No. 44787/98 (2001), para. 56.
[17] Ibid. (citing additional references).
[18] See e.g., Niemietz v. Germany, App. No. 13710/88 (1992).

context, which may fall within the scope of 'private life'."[19] Inevitably, the protection of private life also often overlaps with the other spheres covered by Article 8—home, family and correspondence.[20]

2.1.2. Justification of Interferences

2.1.2.1. ICCPR

The text of the ICCPR does not list any permissible limitations to Article 17. Thus, a plain reading of the text alone suggests that only interferences which are neither unlawful nor arbitrary are justified. Joseph et al., however, contend that Article 17 should likely be understood as having limitations "very similar to the enumerated limits found in other ICCPR guarantees."[21] Accordingly, they suggest that measures that infringe Article 17 may be justified if they are "necessary in a democratic society" which entails "notions of reasonableness and proportionality."[22] This view accords with General Comment 16 which indicates that interferences authorized by law must be "reasonable in the particular circumstances."[23]

General Comment 16 also indicates that the prohibition against "unlawful" interference denotes that any interference must be supported by law and adds that any legal authorization that may exist must conform with the "provisions, aims and objectives of the Covenant."[24] The prohibition against "arbitrary interference", according to the Comment, likewise indicates that even interference sanctioned by law must comport with the aims of the Covenant and be "reasonable in the particular circumstances."[25] The Comment itself may offer a suggestion of what "reasonable in the particular circumstances" means[26]: paragraph 7 states that state authorities should only be able to request information pertaining to an individual's private life where that information "is essential in the interests of society as understood under the Covenant."

2.1.2.2. ECHR

Article 8(2) of the ECHR provides conditions under which state interference with the right to respect for private life is permissible: The interference must be 1) "in accordance with the law"; and 2) "necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of

[19] P.G. & J.H. v. the United Kingdom, para. 56.
[20] K. Reid, *A Practitioner's Guide to the European Convention on Human Rights*, 3rd edn. (London: Sweet & Maxwell, 2007), p. 481
[21] Joseph, Schultz and Castan, supra note 3, p. 483.
[22] Ibid., p. 484.
[23] Para. 4.
[24] UN Human Rights Committee, supra note 4, para. 3.. It is unclear whether this latter clarification is meant to modify the term "unlawful" or reflects the added prohibition against *arbitrary* interference. Cf. Joseph, Schultz and Castan, supra note 3, p. 482, para. 16.11.
[25] UN Human Rights Committee, supra note 4, para. 4.
[26] Joseph, Schultz and Castan, supra note 3, p. 483. (also citing the HRC opinion *Toonen v. Australia* (488/92) at para. 8.3 ("The Committee interprets the requirement of reasonableness to imply that any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case")).

others." Thus, whenever government action that interferes with the right to respect for private life is challenged before the ECtHR, the Court will assess whether these two requirements are met.

Under the first prong of this examination, the Court is interested not only in establishing whether the government body had legal authority under national law to take the action (legal basis) but also in evaluating the "quality" of that authority.[27] The Court has indicated that this qualitative analysis includes appraising whether the law permits citizens to foresee under what circumstances they may become subject to government interference as well as the question of whether the law is generally compatible with the rule of law.[28] Additionally the measure must pursue a legitimate aim,[29] although the Court seems to treat this requirement as a separate one which does not belong definitively to either prong. The second prong of the test has been primarily associated with proportionality—assessing whether the impact on human rights which the government action in question represents is justified in light of the aim that action seeks to achieve. However, the Court has articulated different formulations of the second prong of the test. In *A, B & C v. Ireland*, the test was articulated as the assessment of "[1] whether there existed a pressing social need for the measure in question and, in particular, [2] whether the interference was proportionate to the legitimate aim pursued, regard being had to the fair balance which has to be struck between the relevant competing interests in respect of which the State enjoys a margin of appreciation."[30] In addition, the Court may assess whether the reasons given to justify use of the measures are "relevant and sufficient".[31] The distinction between the two prongs, however, is not always clearly maintained. In a number of cases, the Court has suggested that the examination of whether a measure was "necessary in a democratic society" could involve a qualitative assessment of relevant law.[32] This circumstance indicates that the provision of checks against abuse and arbitrary intrusion that are provided by law play a role in assuring that government powers are exercised in a manner proportionate to the harms to which those powers are addressed.

In Accordance with the Law

In cases before the ECtHR that have concerned search, seizure, and surveillance, the conformity of the measure in question with Article 8 of the ECHR has generally hinged on the first factor (in accordance with the law).[33] Thus, the Court concerns itself with assessing

[27] P.G. & J.H. v. the United Kingdom, App. No. 44787/98 (2001), para. 44.
[28] Ibid.
[29] Peck v. United Kingdom, App. No. 44647/98 (2003), paras. 64-67.
[30] A, B & C v. Ireland, App. No. 25579/05 (2010), para. 229 (with additional citations).
[31] See *Peck,* para. 76. See also P. de Hert, "Balancing Security and Liberty Within the European Human Rights Framework: A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies After 9/11" (2005) 1, Utrecht Law Review, 68–96 at 91–2.
[32] In the seminal case of *Klass*, for instance, although the Court's discussion is couched in terms of the second requirement of Art. 8(2), it is concerned with examining the adequacy of the safeguards provided by the German surveillance law then in force. See generally, Klass & Others v. Germany, App. No. 5029/71 (1978). More recently, in the case of Aleksanyan v. Russia, the Court stated that "[t]o determine whether these measures were 'necessary in a democratic society', the Court has to explore the availability of effective safeguards against abuse or arbitrariness under domestic law and check how those safeguards operated in the specific case under examination." Aleksanyan v. Russia, App. No. 46468/06 (2008), para. 214. See also infra note 79.
[33] Accord de Hert, supra note 31, p. 91 ("In our opinion the Strasbourg judges are too hesitant and reluctant to apply this check and they clearly prefer the much more secure testing of the legality requirement (is there a law?).").

whether regulation is in place that authorizes and governs the state interference and whether that regulation is sufficiently definite and provides adequate safeguards. In this context, the Court has expressed particular concern when authorities engage in "secret surveillance". The Court accepted in *Klass*, that the exercise of powers of secret surveillance "is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime."[34] There, the Court specifically acknowledged the "development" of terrorism in Europe as one factor that justified resort to such measures. *Klass*, however, also made clear that "adequate and effective guarantees against abuse" had to be in place.[35] Similarly in the *Malone* case, the Court noted that "[s]ince the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large", national law had to "indicate the scope of . . . discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."[36] *Klass* provided reference to specific considerations of relevance for the determination of whether national law provided sufficient safeguards: 1) the nature, scope, and duration of possible surveillance measures; 2) the grounds on which those measures would be permitted; 3) the particular authorities that were given the power to carry out and supervise the measures; and 4) the nature of any remedies provided to the subjects of surveillance.[37] In *Kruslin* and *Huvig*, two cases which concerned wiretapping, the ECtHR named specific deficiencies in the national surveillance law which indicated that the law could not be deemed to provide adequate protections against abuse.[38] These deficiencies were reformulated in *Weber and Saravia v. Germany* and presented as "minimum safeguards", indicating that they are now regarded as mandatory protective measures to be included in national regulation of communications surveillance. These were:

1) definition of the nature of offences for which surveillance measures are permitted;
2) definition of the categories of persons who may become subject to such measures;
3) limits on the duration of surveillance;
4) procedures for examining, using, and storing data from the surveillance;
5) the precautions to be taken when communicating data to other parties;
6) the circumstances for the destruction of recorded information from the surveillance.[39]

The *Liberty* case[40] provides another example of legislation that was found to be inadequate. There, the measures implemented by the UK were found not to be in accordance with the law since the controlling legislation was not sufficiently precise. The Court was also troubled by the wide discretion that was vested in the Secretary of State in terms of providing safeguards and ensuring that they were complied with. As presented to the Court, authorization for surveillance required a warrant that would describe the communication channel to be tapped plus a certificate, which described the categories of information that

[34] *Klass*, para. 48.
[35] *Klass*, para. 50.
[36] Malone v. the United Kingdom, App. No. 8691/79 (1984), para. 68. See also Bykov v. Russia, App. No. 4378/02 (2009), para. 78.
[37] *Klass*, para. 50.
[38] See Kruslin v. France, App. No. 11801/85 (1990), para. 35; Huvig v. France, App. No. 11105/84 (1990), para. 34.
[39] Weber & Saravia v. Germany, App. No. 54934/00 (2006), para. 95.
[40] Liberty and Others v. the United Kingdom, App. No. 58243/00 (2008).

would be extracted from the intercepted communications.[41] Both documents, as a rule, would be issued by the Secretary of State.[42] Warrants permitted interception of broad categories of communications, e.g. all communications travelling on commercial submarine cables between the UK and Europe.[43] The Secretary of State had the sole discretion in making the determination of which intercepted communications should be examined. Allegations presented to the Court suggested that vague criteria were used such as "all communications implicating national security."[44] Safeguarding of disclosure and reproduction of captured communications as well as observance of the certificate also fell solely to the Secretary of State, who was granted broad discretion to implement measures "as he consider[ed] necessary".[45] Lastly, whereas the German G10 law at issue in the *Weber* case contained provisions relating to procedures, in the UK, procedures were prescribed in internal rules and policies which were not publicly available nor produced for the Court.[46]

Necessary in a Democratic Society

Government action has been found to fail the second prong of the test in cases involving searches conducted by the police where the warrant obtained to authorize the search was deemed to be worded too vaguely.[47] This put too much discretion in the hands of the authorities conducting the search. In *Aleksanyan v. Russia*, the ECtHR provided explicit factors to be considered in evaluating whether a particular search met the requirement of necessity. Those were: "the severity of the offence in connection with which the search and seizure have been effected, whether they were carried out pursuant to a warrant issued by a judge or a judicial officer – or subjected to after-the-fact judicial scrutiny –, whether the warrant was based on reasonable suspicion and whether its scope was reasonably limited"; "the manner in which the search was executed"; and the "the possible repercussions on the work and the reputation of the persons affected by the search".[48]

In the *Weber* case, the Court indicated that the examination of whether the measures were "necessary in a democratic society" concerned "whether the interferences in question were proportionate to the legitimate aim pursued".[49] Here, many of the same limitations and safeguards that were considered relevant for the examination of whether the measures were in accordance with the law were also considered dispositive for the question of necessity. First, the Court noted that the statute only authorized strategic monitoring for a limited number of offences and that these offences represented "serious criminal acts".[50] Additionally, only the President of the Federal Intelligence Service or his or her deputy could request such surveillance and had to submit a written application which provided the reasons that justified the monitoring.[51] The application had to be approved by a Federal Minister or, as the case may be, the highest authority of the relevant regional government (*Land*) as well as a special Parliamentary Supervisory Board.[52] An additional commission (the

[41] Ibid., para. 43.
[42] Ibid., paras. 25 & 43.
[43] Ibid., para. 64.
[44] Ibid., para. 65.
[45] Ibid., para. 66.
[46] See ibid., paras. 66-68.
[47] Smirnov v. Russia, App. No. 71362/01 (2007); Iliya Stefanov v. Bulgaria, App. No. 65755/01 (2008); Aleksanyan v. Russia, App. No. 46468/06 (2008).
[48] *Aleksanyan*, para. 214 (with additional citations).
[49] *Weber*, para. 107.
[50] Ibid., para. 115.
[51] Ibid.
[52] Ibid.

"G10 Commission") had to authorize the measures either before implementation, or in exigent circumstances, after the fact.[53] This procedure, the Court opined, "ensure[ed] that measures were not ordered haphazardly, irregularly or without due and proper consideration."[54] The Court also noted the safeguards and limitations that were imposed while monitoring measures were in place. Surveillance had to cease immediately once the conditions required by the statute were no longer met or the measures were no longer necessary.[55] The Court characterized the three-month limit on monitoring as "fairly short".[56] The German Federal Constitutional Court had additionally ordered that data obtained through strategic monitoring be clearly marked as such and not used for any purposes other than those outlined in the statute.[57] The statute imposed limitations on the sharing of the data with other authorities and imposed procedures for the retention and destruction of data as noted above.[58] With respect to the oversight mechanisms for strategic monitoring, the Court took special notice of the fact that the Parliamentary Supervisory Board had to include members of the current opposition party and was entitled to receive periodic reports on ongoing surveillance measures from the Federal Minister.[59] It also found that the G10 Commission "had substantial power in relation to all stages of interception."[60]

The Court also examined the sharing of data garnered from strategic surveillance as permitted under German law as modified by a decision of the German Federal Constitutional Court. The applicants who had brought the action complained that sharing of personally identifiable data with other federal agencies in relation to offences specified in provision (3) of the G10 statute could be abused for political purposes.[61] The Court, however, was satisfied that the conditions imposed by the German Federal Constitutional Court—that the data only be transmitted pursuant to the original purposes for which the data were collected—provided sufficient protection against abuse.[62] The Court also accepted the German government's argument that sharing of personally identifiable data as opposed to anonymized data "might prove necessary" to avert the dangers for which strategic monitoring had been authorized through the statute.[63] One provision of the G10 statute permitted provision of data to the Offices for the Protection of the Constitution under certain circumstances.[64] The decision as to whether sharing of the data under these circumstances was called for was taken by an officer qualified for judicial office.[65] The offences for which such sharing was possible included less serious offences such as public fraud.[66] The applicants complained that sharing personal data "obtained by means of a serious interference with the secrecy of communications to combat a multitude of offences—some of which were rather petty—even if they were only in the planning stage" violated the principle of proportionality. The Court found that "the transmission of personal data obtained by general surveillance measures without any specific prior suspicion in order to allow the institution of criminal proceedings against those being monitored constitutes a fairly serious interference with the right of these persons to secrecy of

[53] Ibid.
[54] Ibid.
[55] *Weber*, para. 116.
[56] Ibid.
[57] Ibid.
[58] Ibid..
[59] Ibid., para. 117.
[60] Ibid.
[61] Ibid., para. 120.
[62] Ibid., paras. 121-22.
[63] Ibid., para. 122.
[64] Ibid., para. 36.
[65] Ibid., para. 37.
[66] Ibid., para. 42.

telecommunications."[67] However, it opined that the limitation of the use of the data to the more serious offences as well as the requirement that destruction of the data be recorded in minutes in accordance with the judgement of the Federal Constitutional Court provided an effective counterbalance to abuse.[68]

Since counter-terrorism data mining does not concern communications alone, it is significant to note that the ECtHR has applied less stringent standards for other forms of surveillance. The case of *Uzun v. Germany* concerned the use of GPS surveillance for a period of roughly three months in an investigation related to a bomb attack. Although the Court found that the surveillance had interfered with the applicant's right to respect for private life, they ruled that the interference was justified. The fact that the national law only permitted GPS surveillance when the investigation involved a criminal offence of "considerable gravity" and that judicial review was available after-the-fact in order to assess the proportionality of the measure provided sufficient safeguards against abuse, the Court determined.[69] Notably, national law provided that the subject of surveillance was to be informed of the surveillance once this could be done without jeopardizing the investigation.[70] Thus, it was more likely that wrongful or illegitimate surveillance would come under court review. Unlike with telephone tapping, there was no requirement that an independent body authorize the measure, therefore the fact that German law provided prosecutors with the discretion to order GPS surveillance without a court order was not a basis for complaint under Article 8.[71] The basis for the discrepancy in treatment of GPS surveillance versus communications surveillance was that "GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings."[72] Thus, the Court deemed that GPS tracking was not as intrusive as visual or communications surveillance and therefore did not require the same level of protection against abuse.

2.2. Implications for Data Mining

2.2.1. Whether There is an Interference with the Right to Privacy

Data mining programmes that utilize personal data clearly represent an interference with the right to privacy. The ECtHR has indicated, for instance, that any collection, storage, and/or processing of data pertaining to individuals represents an interference with the right to respect for private life.[73]

[67] Ibid., para. 125.
[68] Ibid., para. 129.
[69] Uzun v. Germany, App. No. 35623/05 (2010), paras. 70-72.
[70] Ibid., paras. 31, 72.
[71] Ibid., paras. 71-72.
[72] Ibid., para. 52.
[73] *Uzun*, paras. 46 & 47 (citing Rotaru v. Romania [GC], App. No. 28341/95, paras. 43-44, ECHR 2000-V; P.G. and J.H. v. the United Kingdom, para. 57; *Peck*, para. 59; Perry v. the United Kingdom, App. No. 63737/00, para. 38); compare also Amann v. Switzerland [GC], App. No. 27798/95, paras. 65-67, ECHR 2000-II).

2.2.2. Whether Any Interference May Be Justified

2.2.2.1. ICCPR

Under the ICCPR, data mining programmes would have to both accord with the aims of the Covenant and represent a measure that was "reasonable in the particular circumstances". There is also some suggestion that the HRC would require that the use of personal data within the scope of the programme be essential in the interests of society as understood under the Covenant. As noted above, the Committee has also indicated that searches of an individual's home should be "restricted to a search for necessary evidence". While it is unclear whether a similar restriction would be imposed on counter-terrorism data mining, the Committee's finding does reflect a requirement that any interference must be tailored to the objective that the measure seeks to further. Thus, one might derive the principle that the impact of a particular data mining programme on the right to privacy must be limited to that which is necessary to achieve the programme's aim. Lastly, the concluding observations of the Committee suggest a preference for the establishment of an independent oversight authority—particularly within the judiciary—over government surveillance activities. Thus, the Committee might impose a warrant or similar requirement for the operation of data mining programmes. Persistent data mining—that is, data mining that continued indefinitely—would be inconsistent with such a requirement. Instead, use of a programme would have to be in response to a specific threat.

2.2.2.2. ECHR

According to the framework established by the ECtHR, a measure that interferes with Article 8 of the ECHR must have a legal basis, pursue a legitimate aim, be foreseeable to those whose rights would be affected, and be compatible with the rule of law. In addition, the measure must be deemed necessary in a democratic society. This requirement may either entail that: 1) there be a pressing social need for the measure and that the interference was proportionate to the legitimate aim pursued, regard being had to the fair balance which has to be struck between the relevant competing interests in which the state enjoys a margin of appreciation; or 2) that the reasons presented to justify the measure be "relevant and sufficient" and the measure be proportionate to the legitimate aims pursued.

In Accordance with the Law

The first prong of the ECHR test entails that data mining programmes must be explicitly authorized by law. The authorization need not take the form of a statute, but the foreseeability requirement necessitates that it be found in a published form of regulation as opposed to an internal set of rules that are not accessible to the public.[74] The law need not permit a particular individual to determine when the authorities are likely to conduct surveillance that will implicate his or her private life; nonetheless, "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered" to use measures that interfere with the right to respect for private life.[75]

[74] See *Liberty*, paras. 59-63.
[75] *Malone*, para. 67.

National law must also provide checks against abuse. Here, there is some divergence between the HRC and the ECtHR. The ECtHR has distinguished between surveillance that involves communications and that which does not. Thus, its jurisprudence suggests that data mining that involves communications or communications data would be held to more stringent standards than other data mining programmes. There is also some suggestion that the Court would subject programmes involving visual data to the more stringent standards.[76] This distinction reflects the fact that the Court deems communications surveillance to entail a higher level of intrusion than, for instance, locational tracking. Thus, the principle of proportionality would suggest that higher standards must be applied where there is potential for a greater level of harm. In those instances in which more stringent standards applied, the law would additionally need to define the "categories of persons" whose data might become subject to the data mining operation, impose limits on the duration of the programme—although a duration of three months would likely be permissible— and provide details pertaining to the handling of data, including the circumstances for destruction of that data. In terms of the "categories of persons" who may be subjected to the measure, the ECtHR looks for specific language in the law that defines whether, for instance, only suspects of specified offences may be targeted or also accomplices, associates, etc. The use of vague language in defining these classes of persons is likely to be found impermissible. Additionally, whether the scope of the affected classes of persons is appropriate would be tested under the necessity prong. Furthermore, any deployment of the data mining programme would require the prior authorization of an independent authority—which could, but need not necessarily take the form of a judge.

Necessary in a Democratic Society

The use of data mining programmes as outlined in the law must pursue a legitimate aim. In light of the ECtHR's findings in *Klass*, the Court would be likely to find the use of data mining to combat terrorism in pursuit of a legitimate aim.

As noted above, the necessity requirement is essentially concerned with the question of proportionality. The examination of proportionality may take on a *substantive* aspect or a *procedural* aspect. In the *S & Marper*[77] case, for instance, the Court held that the retention of fingerprints, cellular samples, and DNA profiles of persons who were merely suspected of involvement in a crime but were not convicted violated the principle of proportionality. Such a measure "failed to strike a fair balance between the competing public and private interests".[78] This represents a more substantive approach in that it assesses the actual interference with the rights of the applicants against the harm that the interfering measure is intended to address. In other cases, the Court concentrates more on whether the existing procedural safeguards effectively limit the scope of interference to such an extent that a fair balance is struck. In the *Weber* case, for example, the Court focussed on the statutory framework that authorized strategic monitoring to assess the legal safeguards and limitations on the use of the measure. Thus, in its discussion of the necessity prong, the Court reviewed many of the same statutory features that it considered dispositive for the assessment of the qualitative requirements of the "in accordance with the law" prong.[79]

[76] See *Uzun*, para. 52.
[77] Application Nos. 30562/04 and 30566/04 (2008).
[78] Ibid., para. 125.
[79] Compare *Weber*, paras. 115-117 and paras. 96-100.

Clearly, safeguards as well as formal limitations on the scope of application of a particular measure can both serve to limit the impact on human rights and thus play a role in maintaining proportionality. Thus, procedures which require government agents to articulate the need for the use of a particular measure and impose review by a supervising authority or a judge before final authorization is granted serve to prevent the occurrence of interferences with human rights without a showing of the appropriate level of justification. Similarly, the limitation of measures to serious offences can ensure that the level of potential harm in terms of human rights only occurs where the gravity of the situation requires it. The imposition of default time limits also places a barrier on initial harm and provides an opportunity for review of the results of the measure to determine if longer resort to its use is justified. Nonetheless, the question arises as to whether the Court would find no violation on the basis of the provision of such procedural safeguards where the human rights impact in terms of the number of individuals whose right to respect for private life had been interfered with could be shown to be on a massive scale. In this regard, the *Weber* and *Liberty* cases are of particular interest.

Both the *Weber* and *Liberty* cases concerned broad surveillance in the form of signals intelligence—in the case of *Liberty*, the alleged interception of telephone, facsimile, and e-mail communications between Ireland and the UK by the UK Ministry of Defence and in *Weber and Saravia*, the performance of "strategic monitoring" by the German Federal Intelligence Service to avert "serious dangers" to national security. In *Liberty,* the applicants alleged that, upon issuance of warrants, the UK government was capturing all communications that were sent along a particular channel and then used a search engine to "filter" out those communications that were likely to be of most interest.[80] It is unclear whether the German measures represented the same scale and form of surveillance. *Weber* indicated that the surveillance in question did not concern monitoring of a particular individual[81] and involved "monitoring" and "recording" of communications.[82] The German legislation (the so-called "G10 Act") also contained provisions governing the use of "catchwords"[83] which could serve the same function as the search engine-driven "filtering" referred to in *Liberty*. Additionally, neither the G10 Act nor *Weber* indicates whether the catchwords were applied before or after communications had been recorded. In any event, even in the most favourable scenario, there would seem to be some risk that communications that did not meet the purpose of the exercise would be intercepted through the use of catchwords.

It is also unclear whether either of the measures in the two cases actually entailed the use of data mining. Neither case explicitly used the term "data mining" but conceivably data mining could be used to perform the sort of filtering function described. Regardless of whether data mining was used, the type of catchword-assisted surveillance reflected in the cases represents an analogous phenomenon. Therefore, the cases provide the most relevant insight into how the Court might deal with data mining, for instance in a profiling manner.

Despite the fact that similar forms of surveillance were at issue in the two cases, the Court found a violation of Article 8 in *Liberty* but no violation in *Weber*. The determining factor was the fact that the German legislation provided safeguards and limitations that the Court

[80] *Liberty*, para. 43.
[81] See *Weber*, para. 18.
[82] *Weber*, para. 19.
[83] Ibid., para. 32. The term used in the Act is "Suchbegriffe" ("search terms"). *G10,* 1 BvR 2226/94 (Bundesverfassungsgericht, 14 July 1999), para. 29. See also Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, § 5(2) (2009).

found to be adequate for purposes of Article 8(2), whereas the surveillance regime permitted under UK law was found to be wanting in this respect. Yet, both cases concerned very broad forms of surveillance. The G10, however, appeared to limit the measure to actual, specific threats, whereas the UK measures seemed more open-ended. On the other hand, the applicants in *Weber* complained that under the revised version of the G10, there were "no longer" any geographic restrictions on the use of such monitoring,[84] suggesting that strategic monitoring could involve tapping communications throughout the world. In contrast, the practice of the UK as presented to the Court in *Liberty* focussed on a particular channel of communication which was geographically limited, although there was nothing to suggest that the UK warrant system might not name multiple communication channels to extend the geographic scope of surveillance.

The full implications of *Weber* are therefore not entirely clear. One possibility is that the Court was cognizant of the broad scale of interference that strategic monitoring could represent, but found that the "pressing need" for which such measures were implemented was so dire that such interference was justified. Additionally, a generous margin of appreciation in matters of national security may also have entered in to the Court's calculus. On the other hand, the case might have had a different result if the Court had been presented with hard figures in terms of the number of individuals whose communications had been subjected to the monitoring. Complainants, however, will generally find it difficult to obtain such hard numbers where "secret surveillance" measures are concerned.

Furthermore, assessing the seriousness of an interference with the right to respect for private life may not be straightforward. Some may argue that examination of communications or abstracts of communications by machines is a relatively minor interference compared to a situation where communications are read by human eyes or listened to by human ears. As we noted in Deliverable 8.2, the same argument may be made with respect to data mining.[85] Thus, some would argue that the fact that data pertaining to hundreds, thousands, or millions of individuals are subjected to a particular data mining programme,[86] potentially on a repeated basis, means that there is a serious interference with Article 8 of the ECHR. On the other hand, others may argue that where such large amounts of data are, in most cases, only scrutinized by machines but not human beings, the interference is not particularly serious. There will be more to say on this issue with regard to the subject of data protection, but the massive scale that is often associated with data mining as well as signals intelligence presents a particularly critical factor for the question of proportionality in privacy law.

In addition to the scale of impact of the measure on human rights, there is also the question of effectiveness. In Deliverable 8.2, we suggested that the actual effectiveness of a measure should also play a role in proportionality analysis.[87] Effectiveness or "suitability" is a recognized element of proportionality analysis under the national law of some European

[84] Ibid., para. 111.
[85] D08.2, Section 5, p. 34.
[86] By way of example, we noted in D8.2 that the *Rasterfahndung* reportedly involved searches against the data of 8.3 million people. D08.2, Section 3.3, p. 12. Since the databases that were searched included residential registries and university databases, the initial searches may have actually been run against the data of all registered residents of the country as well as any non-residents who were enrolled as university students. Thus, the full range of processing of personal data may have affected a much larger number of individuals. Data mining programmes proposed in the area of aviation security would at least involve processing the data of all individuals who enter, depart from, and potentially transit through the country hosting the programme.
[87] Ibid, p. 3.

states and in the jurisprudence of the ECJ. However, effectiveness or suitability in the legal sense appears to be a very low hurdle, which does not seek to assess the actual effectiveness of a measure in achieving its intended aim, but rather tests to ensure that a measure is not wholly unsuited on its face.[88] Thus, if the measure could conceivably further the achievement of the goal in any way, it would seem to generally meet the effectiveness requirement.[89] The consideration of actual effectiveness may rather fall under the legal concept of necessity and has appeared in the jurisprudence of the ECtHR.[90] A measure which interferes with the right to respect for private life but which accomplishes little cannot be considered "necessary" in any sense for the achievement of the intended aim.

Tied to the concept of necessity in proportionality analysis is the principle which is often referred to as "subsidiarity". Subsidiarity requires that, whenever measures will impact human rights, governments adopt the least intrusive measures available to achieve the particular objective sought. This requirement has been applied by the ECtHR in proportionality analysis.[91] As we suggested in D8.2, less intrusive means of combating terrorism than large-scale data mining programmes, including more limited applications of data mining, may not only suffice to achieve the objective of countering terrorism but may also be more effective.

Thus, for a number of reasons, large-scale counter-terrorism data mining programmes are unlikely to meet the requirement of proportionality. Such data mining programmes could not be regarded as "necessary in a democratic society" for the prevention of terrorism.

3. Data Protection

Data protection law represents a subset of privacy law that concerns the handling of personal data. It seeks to ensure that privacy is protected in the processing of data relating to individuals, and is reflected in a number of instruments at both the European and international level.

The most important instrument at the international level is the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. As the title "Guidelines" suggests, the language of the instrument is aspirational and does not represent a legally binding instrument.

---

[88] See Schwarze, J., *Europäisches Verwaltungsrecht: Entstehung und Entwicklung im Rahmen der Europäischen Gemeinschaft* (Baden-Baden: Nomos-Verl.-Ges., 1988), p. 833; In the *Jippes* case, the ECJ determined that state action is disproportionate where the measure applied is "manifestly inappropriate in terms of the objective which the competent institution is seeking to pursue". Case C-189/01, Jippes (2001) ECR I-5689, para. 82.

[89] In the *Rasterfahndung* case before the German Constitutional Court, for instance, the question of suitability was glossed over, suggesting that the Court considered the criterion to have obviously been met, despite the fact that the exercise did not prove to be effective at all.

[90] For instance, in the case Observer and Guardian v. UK, App. No. 13585/88 (1991), in the context of Article 10 of the ECHR, the Court found that measures which could no longer serve to further their intended aim could no longer be deemed to be "sufficient". Paras. 68-69. Consideration of actual effectiveness may also be reflected in Article 52 of the Charter of Fundamental Rights of the European Union in that it requires that limitations to Charter rights "*genuinely* meet objectives of general interest recognised by the Union" (emphasis added).

[91] See Informationsverein Lentia and Others v. Austria, App. Nos. 13914/88, 15041/89, 15717/89, 15779/89, 17207/90 (1993), para. 39.

At the European level, the most relevant instrument is the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Although it provides similar protections as those included in the OECD Guidelines, as the title of the Convention implies, it relates specifically to personal data that is subject to automatic processing and is thus narrower in scope. The Convention, however, provides the possibility for member states to declare that they will apply the Convention also to the handling of personal data that does not involve automatic processing.[92] "Automatic processing" is defined in the Convention as the "storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination" where those operations are carried out in any part through automated means.[93] The Committee of Ministers of the Council of Europe also adopted a resolution in 1987 which provides data protection principles for the automated use, handling, and processing of personal data within the police sector.[94]

At the level of the European Union, the Charter of Fundamental Rights of the European Union establishes a right to the protection of personal data in Article 8. This article provides that personal data may only be processed with the consent of the data subject or where legitimately authorized by law.[95] Additionally, the processing must be done "fairly" and for a specified purpose.[96] Article 8 also establishes that every person has the right to have access to personal data that pertains to him or her and to have that data corrected.[97] Lastly, it requires that member states have a national authority to ensure compliance with Article 8. The quintessential law for data protection within the European Union is the EU Data Protection Directive.[98] The directive represents the effort to establish a harmonized regime of minimum standards of data protection throughout the Union. It draws upon principles established in the OECD Guidelines and the Council of Europe Convention and shares many similarities with the Convention in particular. Also of relevance for counter-terrorism data mining is the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[99] The Framework Decision applies to personal data transferred between or among member states or to non-member states for law enforcement purposes and includes coverage of data made available to information systems established on the basis of Title VI of the Treaty on European Union.[100] Like the Directive, the Framework Decision applies both to automated processing and non-automated processing.[101]

The jurisprudence of the ECtHR on the right to respect for private life also reflects data protection principles in that it incorporates them into this right. There is thus some evidence that actions that violate data protection principles will be held to represent an interference with Article 8 of the ECHR. The case of *S & Marper v. UK*, for instance, made

[92] Art. 3(2)(c).
[93] Art. 2(c).
[94] Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector (1987).
[95] Art. 8(2).
[96] Ibid.
[97] Ibid.
[98] 95/46/EC.
[99] 2008/977/JHA.
[100] Art. 1(2). In the original version of the treaty, Title VI referred to provisions concerning police and judicial cooperation in criminal matters. These were later moved to Chapters 1, 4 and 5 of Title V of Part Three of the Treaty on the Functioning of the European Union. See Tables of Equivalences, C 83/364 (30.3.2010).
[101] Art. 1(3).

numerous citations to the Council of Europe's Data Protection Convention,[102] indicating that the Court will also enforce that Convention through the ECHR. In that case, the Court stated that the "mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8"[103] and that "protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention."[104] A number of cases have also found the collection and storage of personal data on the part of law enforcement or national security services to constitute an interference with Article 8.[105] As noted above, issues pertaining to the retention, handling, sharing, and destruction of data as well as the provision of notice to affected data subjects were significant considerations in the *Weber* and *Liberty* cases.

As noted above the ECtHR has indicated that it may refer to the Convention on Automated Processing in the application of Article 8 of the ECHR. Thus, the Court may interpret an interference with data protection rights under that Convention as an indication of an interference with the right to respect for private life under Article 8 of the ECHR. This would implicate data mining that involves the processing of data that pertains to an identified or identifiable individual.

3.1. Exceptions and Derogations

A central issue for the relevance of data protection law for counter-terrorism data mining is the inclusion within international instruments of opportunities for states to derogate from provisions of the respective instrument, particularly with regard to matters of national security and/or criminal law enforcement, as well as the outright exclusion of the instrument's application in the areas of national security, intelligence, or criminal law enforcement.

The OECD Guidelines, for instance, appear to permit exceptions to the principles or to the promotion of the free flow of data in paragraph 4. However, such exceptions "including those relating to national sovereignty, national security and public policy" should be "as few as possible" and "made known to the public".

The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data permits member states to derogate from the provisions pertaining to data quality, special categories of data, and the right to request information or seek rectification of data. In order to do so, however, the derogation must be "provided for by the law of the Party" and represent "a necessary measure in a democratic society in the interests of... protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences" or "protecting the data subject or the rights and freedoms of others."[106] Member states may, at any time, also exclude certain categories of data from the application of the Convention by making a declaration to the Secretary General of the Council of Europe and depositing a list of the categories to be

[102] See, e.g., paras. 103-04.
[103] Para. 67.
[104] Para. 103.
[105] Uzun v. Germany; Rotaru v. Romania, App. No. 28341/95 (2000); P.G. and J.H. v. the United Kingdom; Peck v. United Kingdom; Perry v. the United Kingdom; Amann v. Switzerland, App. No. 27798/95 (2000).
[106] Article 9(2).

excluded.[107] Some member states have made declarations under this provision that exclude the processing of data for purposes of law enforcement or national security.[108]

Article 3(2) of the EU Data Protection Directive provides that the Directive shall not apply "to processing operations concerning public security, defence, State security, and the activities of the State in areas of criminal law". Article 13 also permits member states to enact additional exemptions to the application of the Directive for purposes of national and public security, defence, and criminal law enforcement and ethics enforcement for regulated professions. These provisions thus allow member states to exclude data mining done in the name of counter-terrorism from the scope of national data protection law and make additional adjustments to that law to accommodate counter-terrorism programmes.

The Framework Decision on police and judicial cooperation also appears to hold some forbearance with respect to its application in areas touching upon national security. Article 1(4) states that the Framework Decision "is without prejudice to essential national security interests and specific intelligence activities in the field of national security."

As noted above, the EU Data Protection Directive provides EU member states with leeway to exempt counter-terrorism activities from data protection since these would fall squarely within the realm of national security, and the EU Framework Decision appears to extend a similar level of discretion at least insofar as the activities fall within the realm of national security measures as opposed to standard law enforcement measures. The Council of Europe's Convention on Automated Processing also permits signatories to derogate from most of the substantive protections provided in the Convention so long as it is "provided for by the law of the Party" and represents "a necessary measure in a democratic society in the interests of... protecting State security". The latter issue would probably be resolved along the lines of the jurisprudence of the ECtHR. Thus, the derogating state would have to be able to show that there is "a pressing social need" and that any interference that results is proportionate to the aim pursued. The need for efficiency in counter-terrorism activities is likely to be viewed as a pressing social need that would justify derogation from the Convention. Whether the derogation is proportionate, however, would depend upon its exact scope. Even if the derogation was limited to counter-terrorism data mining activities, this might not meet the proportionality requirement due to the often overbroad impact of data mining. In any event, Article 8 of the EU Charter of Fundamental Rights as well as the soft principles of the OECD Guidelines would still apply in addition to any data protection principles that form an integral part of Article 8 of the ECHR. Article 8 of the Charter is also subject to limitation. Article 52 of the Charter states that limitations of any of the rights of the Charter must be provided by law and respect the essence of those rights and freedoms. Additionally, they must be "necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others", "[s]ubject to the principle of proportionality".

3.2. Basic Principles

[107] Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Art. 1 (amending Article 2 of the Convention).
[108] See List of declarations made with respect to treaty No. 108, Treaty Office at http://conventions.coe.int (in particular declarations from Andorra, Ireland, Romania, and Malta).

The OECD Guidelines establish eight basic principles of data protection which are also reflected in the legal instruments at the European level. These are 1) collection limitation, 2) data quality, 3) purpose specification, 4) use limitation, 5) security safeguards, 6) openness, 7) individual participation, and 8) accountability. Additionally, the Guidelines introduce three central concepts for the regulation of data protection, namely that of the "data controller", "personal data" and the "data subject". A "data controller" as defined by the Guidelines is an authority established under national law who determines the content and use of a collection of data. A data controller need not actually be involved with the collection, storage, and processing of the data.[109] "Personal data" is defined as "any information relating to an identified or identifiable individual".[110] A "data subject" is the individual to whom data (the personal data) in a collection pertain.[111] The following sections discuss in further detail the data protection principles.

3.2.1. Collection Limitation

The collection limitation principle establishes that there "should be limits to the collection of personal data" and that the collection of data should take place through lawful and fair means and "where appropriate with the knowledge or consent of the data subject."[112] The EU Data Protection Directive includes collection within the meaning of "processing".[113] Therefore, all limitations that apply to processing under the Directive would also apply to collection.

The collection limitation principle may have direct implications for counter-terrorism data mining in two ways. First, where data mining programmes perform aggregating functions or pull data from sources that are not under the direct control of the data controller, these programmes may be seen as performing data collection. Second, if one adopts a broad definition of the term "collection", data mining programmes that in the course of their operation copy or store data in new locations may also be viewed as "collecting" data. Even apart from these considerations, the limitation of collection is an issue of at least indirect consequence for data mining since many programmes will rely on databases that are either created and maintained to support the programme or were initially created for some other purpose.

The language of the principle that there "should be limits" implies that any collection of data should not go beyond what is necessary for the effective operation of the programme. Data collection should not be done in any manner which would violate existing law, including applicable provisions of the Convention on Automatic Processing as well as the ECHR. The notion that collection should be carried out through "fair means", coupled with the openness and purpose specification principles (discussed below), suggest at a minimum that individuals should be informed that their data is being collected for use in a particular programme. Given that data collection represents the point of departure from which future infringements of human rights may follow, observation of the collection limitation principle is a critical means for limiting the impact of governmental data processing activities.

[109] Para. 1.
[110] Ibid.
[111] Ibid.
[112] Para. 7.
[113] Art. 2(b).

3.2.2. Data Quality

Data quality as defined in the OECD Guidelines stands for the principle that any personal data processed should be relevant to the intended use and be accurate, complete, and up-to-date "to the extent necessary" for the intended use.[114] Both the Council of Europe's Convention on Automatic Processing and the EU Data Protection Directive similarly provide that personal data that is subjected to automatic processing must be "accurate, and, where necessary, kept up to date."[115] The Directive additionally imposes the obligation that states take "every reasonable step" to ensure that inaccurate or incomplete data are erased or corrected.[116] The Framework Decision on police and judicial cooperation obligates relevant authorities to correct inaccurate data and complete or update data where possible and necessary.[117] These authorities must also verify the accuracy of data before transmitting or making it available to their counterparts in other member states.[118] If it becomes known after the fact that data sent or made available to other authorities is inaccurate, the receiving authorities must be informed "without delay".[119] The Framework Decision also imposes the obligation upon recipient authorities to correct, delete, or otherwise limit the further processing of such data.[120]

The issue of data quality and the problems it can produce for data mining was discussed in D8.2. There, we pointed out how data quality issues can hamper the effectiveness of a programme and lead to human rights violations through the occurrence of false positives. Apart from these considerations, the data quality principle provides independent grounds for ensuring the accuracy of data that is used for data mining purposes, which in some instances will rise to the level of an obligation. The Convention on Automatic Processing permits states to derogate from its data quality provisions for state security purposes,[121] which may also be applicable to counter-terrorism data mining. However, any derogation would be subject to the principle of necessity. Thus, governments would have to be able to demonstrate that application of the data quality provisions under Article 5 would hamper efforts to ensure state security. However, as revealed in D8.2, it is the failure to ensure data quality, rather than enforcement of data quality, which will normally hamper state security efforts. There may be instances in which the exigency of the situation would render quality control impractical. Such situations, however, might qualify as a state of emergency in which limited exception to human rights obligations would be permissible but only for the duration of the emergency.[122] They would not provide grounds for a general derogation.

3.2.3. Purpose Specification

Purpose specification means that the purposes for which the data are to be used should be disclosed by the time of collection of the data. It also entails that any use or subsequent use of that data should remain tied to that purpose or purposes or "such others as are not

[114] Para. 8.
[115] Convention, Art. 5(d); Directive Art. 6(1)(d).
[116] Art. 6(1)(d).
[117] Art. 4(1).
[118] Art. 8(1).
[119] Art. 8(2).
[120] Ibid.
[121] Art. 9(2).
[122] See Scheinin and Vermeulen, D06.1, Sec. 3.10.

incompatible with those purposes".[123] Any alteration of purpose should be notified. This principle is also reflected in the European Charter which requires that processing be done "fairly" and for a specified purpose.[124] The Council of Europe's Convention on Automatic Processing incorporates the purpose specification principle in Article 5, which provides that any personal data that is subjected to automatic processing must be "stored for specified and legitimate purposes and not used in a way incompatible with those purposes".[125] The EU Framework Decision also imposes the purpose specification requirement in the context of data transferred between law enforcement or judicial authorities. Article 3(1) of that instrument provides that "[p]ersonal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected." The provision further requires that any processing be "lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected."

Purpose specification is a particularly salient issue for counter-terrorism data mining since the purpose of such programmes is often ill-defined. In some instances, the programme may take the form of a research or investigatory tool rather than a programme with a single, well-defined objective. Additionally, data mining programmes are sometimes designed to make use of pre-existing databases which may have been established for different purposes. The purpose specification principle requires that any such change in the objectives for which personal data are used must be announced through some form of public notice, particularly when the new purpose is one which is "incompatible" with the previously given purpose. The use of databases established for criminal law enforcement purposes in counter-terrorism data mining may be considered compatible purposes. However, the use of databases that were established for purposes not related to criminal law enforcement, such as residential registries, driver registries, or tax registries would not be compatible with counter-terrorism.[126] The purpose specification principle of the Convention on Automatic Processing is contained in a derogable provision, and governments may wish to derogate in this respect with regards to counter-terrorism data mining in order to provide more flexibility. Again, such derogation would only be permissible to the extent necessary. Thus, states would have to show that complying with the purpose specification requirement of the Convention would hinder their counter-terrorism efforts. Furthermore, the purpose specification requirement of the EU Charter would still apply, subject to permissible limitations. Thus, the Charter would require that states explicitly define the purpose of any data mining programme that makes use of personal data unless they could demonstrate that it was necessary to refrain from doing so and that this was consonant with the principle of proportionality and was genuinely effective.

3.2.4. Use Limitation

The use limitation principle of the OECD Guidelines establishes that personal data should not "be disclosed, made available or otherwise used" for any purpose other than that specified unless the data subject gives consent or it is authorized by law.[127] As such it goes hand-in-

[123] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, para. 9.
[124] Art. 8(2).
[125] Art. 5(b).
[126] However, some registries represent public records and some countries have made declarations to exclude the application of the Convention to publicly available information. See List of declarations made with respect to treaty No. 108, Treaty Office at http://conventions.coe.int.
[127] OECD Guidelines, para. 10.

hand with the purpose specification principle and is reflected in the EU Charter, the Council of Europe's Convention on Automatic Processing and the EU Framework Decision as described above.

3.2.5. Security Safeguards

The security safeguards principle of the OECD Guidelines establishes that personal data should be secured against "loss or unauthorised access, destruction, use, modification or disclosure" or other such risks.[128] This principle is also reflected in Article 7 of the Council of Europe's Convention on Automatic Processing which requires that "[a]ppropriate security measures" be taken against the "accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination" of personal data stored in automated data files. The Convention on Automated Processing additionally requires the establishment of "appropriate safeguards" in national law for the automated processing of sensitive data.[129] The EU Framework Decision also applies this requirement to sensitive data when transferred between authorities in different states.[130]

The OECD Guidelines and the Council of Europe's Convention appear to speak primarily to the establishment of technological safeguards and system security whereas the provisions on the protection of sensitive data in the Convention and Framework Decision refer to the creation of legal safeguards. Ideally, both kinds of safeguards should be in place to secure the "physical" integrity of data as well as to ensure that those handling such data do so in a manner that does not compromise the use of that data or expose it to the risk of unauthorized use.

The creation of safeguards against loss, destruction, or modification of data reinforces the principle of data quality since such events can prevent the proper or effective operation of data mining operations that rely on that data. The requirement to provide security against unauthorized access and dissemination not only calls for the implementation of robust access controls in connection with the information systems that provide access to users, but also for the limitation of access to reduce the risk of unauthorized dissemination. Moreover, security measures should not only address the risk of unauthorized access but also of misuse of data on the part of those who have authorized access. A system which automatically creates logs of users' use of the system provides the opportunity for audits—whether manual or automated—to assess whether the system has been misused or compromised. Although the provision pertaining to sensitive data in the Council of Europe's Convention is derogable, Article 7, pertaining to security measures in general, is not.

3.2.6. Openness

The openness principle provided by the OECD Guidelines calls for "a general policy" of transparency with respect to "developments, practices and policies" pertaining to personal data.[131] Furthermore, according to this principle, individuals should be enabled to determine the existence and nature of a collection of personal data, the purposes of their

[128] OECD Guidelines, para. 11.
[129] Art. 6.
[130] Art. 6.
[131] OECD Guidelines, para. 12.

use, as well as the identity and "usual residence" of the responsible data controller. Similarly, the Council of Europe's Convention on Automatic Processing requires states to ensure that the existence of a collection of data that is subject to automatic processing, its "main purposes", and the identity and address of the respective data controller are all ascertainable by any person.[132]

The openness principle reinforces the purpose specification requirement in that it calls on states to reveal the purpose of a particular data processing operation or collection of data. Additionally, information pertaining to changes in the purpose or use of such an operation or data collection should also be available to the public. In order to meet obligations under the Convention, states might, at a minimum, announce details concerning data mining programmes in a government bulletin.[133] However, providing information through media which individuals, particularly in the case of non-citizens, are more likely to encounter or refer to when confronted with the activities of particular agencies that are engaged in counter-terrorism data mining—such as agency websites or pamphlets or notices that are provided at data collection points (border checks, airports, banks or money order businesses) or the public areas of agency offices— might prove more effective.

3.2.7. Individual Participation

The individual participation principle of the OECD Guidelines calls for the recognition of a number of rights for data subjects. First, each data subject has the right to request his or her data from a data controller or otherwise to confirm whether the data controller holds data relating to him or her. Second, that data should be provided to the data subject in an intelligible form, within a reasonable time, in a reasonable manner, and at no excessive cost. Third, in the event that a request for information is denied, the data subject should have the right to receive notice of the grounds for that denial and the opportunity to challenge that denial. Fourth, the data subject should have the right to challenge data pertaining to him or her and have that data erased, corrected, completed, or amended.[134] The Council of Europe Convention confers similar rights under Article 8, whereas the EU Charter merely provides the right to have access to one's own personal data that pertain to him or her and to have that data corrected.[135]

The observance of these rights would likely prove controversial in many instances, since states may be reluctant even to divulge what data is being utilized in data mining programmes for fear that it will aid circumvention of the programme, let alone provide evidence of a potential instance of wrongdoing. States may derogate from the provision of these rights under the Council of Europe Convention, subject to the principle of necessity. Similarly, the more basic EU Charter rights could only be limited to the extent such limitations are "necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others", "[s]ubject to the principle of proportionality".[136] Again, the aim of protecting national security is likely to be viewed as a legitimate objective. However, it seems less likely that the principle of proportionality would permit the outright denial of the right to access and correction for all

[132] Art. 8.
[133] Compare Detailed Comments to the OECD Guidelines, Paragraph 12, ¶ 57.
[134] Para. 13.
[135] Art. 8(2).
[136] Art. 52.

time. Knowledge of the type of data that is subjected to data mining seems too trivial when weighed against the possibility of circumvention.

There is the very real possibility that the revelation of information to individuals will undermine the purpose of a given data mining operation or ongoing investigations. Limitation of the rights described above in such instances may, in the case of the EU Charter, be necessary to meet an objective of general interest and thus be permissible. Where ongoing investigations are no longer endangered, the limitation would no longer be permissible and full observance of the rights would have to be restored. States could also derogate from granting Article 8 rights under the Council of Europe Convention, but the principle of necessity would require the derogation to be limited to denials which are truly required for the protection of state security, public safety or the execution of criminal law enforcement.

3.2.8. Accountability

Lastly, the accountability principle entails that data controllers should be held accountable for observing the principles of the OECD Guidelines.[137] The Council of Europe Convention provides measures for accountability by requiring state parties to provide "appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection" represented in Articles 5 through 8.[138] Article 8 additionally requires states to provide a remedy for individuals where the individual's request for information on, copies, correction, or erasure of personal data has not been complied with.[139] The EU Charter ensures accountability by requiring that member states have an independent authority to ensure compliance with Article 8.

States may comply with Article 8 of the EU Charter by assigning oversight of the observance of data protection rights with respect to counter-terrorism data mining to the national data protection supervisor or equivalent authority. However, in order to avoid overburdening the data protection authority or in light of the particularly sensitive nature of counter-terrorism activities, states may choose to assign these duties to a different authority. Particularly where a significantly different body of national data protection law applies to counter-terrorism activities, the establishment of a separate body may be appropriate. This authority, however, as the Charter clearly establishes, must be truly independent. The provision of remedies to individuals as provided in the Council of Europe Convention may be limited to the extent that states may permissibly derogate from Article 8 or Articles 5 or 6. However, at the very least, states would still need to have a system of sanctions in place for violations of applicable substantive provisions as well as appropriate measures for remedying violations of data security under Article 7.

3.3. Additional Requirements

3.3.1. Permitted Processing

[137] OECD Guideline, para. 14.
[138] Art. 10.
[139] Art. 8(d).

Data protection instruments also define boundaries within which processing of personal data may take place. The EU Charter establishes that personal data may only be processed with the consent of the data subject or where legitimately authorized by law.[140] Processing must also be done fairly and lawfully as provided by both the Charter and the Council of Europe Convention.[141] In addition to consent, which must be given unambiguously, the EU Data Protection Directive outlines the instances in which processing may be authorized by law within the European Union: 1) where the processing is necessary in connection with a contract to which the data subject is a party or wishes to enter into; 2) where the processing is necessary to comply with a legal obligation; 3) where the processing is necessary to protect a vital interest of the data subject; 4) where the processing is necessary as a matter of public interest or to perform an official function; or 5) where the processing is necessary for the pursuit of the data controller's "legitimate interests" except where overridden by the interests of the data subject's fundamental rights and freedoms.[142]

Although the requirements of the EU Data Protection Directive may not apply in the area of counter-terrorism data mining regardless of whether it falls within the realm of law enforcement or national security, they nonetheless serve as an indication that the spirit of data protection law stands for the principle that processing of personal data be limited by certain conditions. An additionally significant aspect of data protection law is the fact that there is no harm requirement. The act of processing personal data in an impermissible manner as such represents a violation of data protection law. This aspect is particularly relevant for data mining, since the vast majority of individuals whose data is subjected to data mining will not experience any harm in the form of enhanced scrutiny from law enforcement or intelligence officials.

Even where national law implementing the EU Data Protection Directive does not apply to counter-terrorism data mining, the EU Charter and potentially the Council of Europe Convention would still require that such data mining be done in a fair and lawful manner. "Lawful" requires not only that the programme conform to relevant legal requirements but also that adequate legal regulation be in place to govern the use of the programme. Additionally, the processing accomplished by the programme would have to be done "fairly". It is not entirely clear what this requirement entails, however, it might mean that the soundness of the programme would have to be demonstrated.

3.3.2. Transfer of Data

Several instruments contain provisions governing the transfer of personal data across borders. The relevant provisions of the OECD Guidelines, in a sense, stand as a kind of counterpoint to the basic principles in that they generally promote the free flow of data internationally. Paragraph 18, for instance, states that "Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection." However, member countries may refuse to allow the transborder transfer of data when the receiving state does not "substantially observe" the Guidelines or where the further transfer of the data would result in the circumvention of the member country's domestic privacy law.

[140] Art. 8(2).
[141] Art. 5(a).
[142] 95/46/EC, Art 7.

Similar to the Guidelines, the Council of Europe Convention on Automatic Processing generally promotes the free flow of data across national borders. Article 12 provides that the transfer of personal data transnationally should not be prohibited or subjected to special authorization solely for the purpose of protecting privacy.[143] However, it permits parties to derogate from this provision insofar as national legislation provides enhanced protection for special categories of data which are not provided in the national legislation of the receiving party.[144] Additionally, derogation is permitted in order to prevent circumvention of the Convention where personal data would be transferred to a state that is not a party to the Convention via a party that is acting as an intermediary.[145]

The EU Data Protection Directive also contains provisions relating to the transfer of personal data outside of the EU. Such transfers may only be allowed when the receiving country provides an "adequate level of protection."[146] However, derogation from this rule is permitted under the same conditions which govern processing generally under Article 7.[147]

The EU Framework Decision includes the right of the data subject to receive information as to whether his or her personal data has been transferred to another state.[148] Receiving states, however, may request that the data subject not be informed of its receipt of his or her personal data without that state's prior consent. Additionally, member states may adopt legislative measures to permit the refusal to provide information where that is a necessary and proportionate measure to prevent the obstruction of legal procedures, to prevent interference with the investigation or prosecution of criminal offences, to protect public or national security, or to protect the data subject or the rights and freedoms of others.[149]

Article 10 of the Framework Decision requires that all transfers of personal data for law enforcement purposes be logged for legal compliance and quality control purposes. The Framework Decision also requires that transfer of personal data to non-member states may only take place where:

> "(a) it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
> (b) the receiving authority in the third State or receiving international body is responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
> (c) the Member State from which the data were obtained has given its consent to transfer in compliance with its national law; and
> (d) the third State or international body concerned ensures an adequate level of protection for the intended data processing."[150]

However transfer to countries that do not offer an "adequate level of protection" may nonetheless take place where:

> "(a) the national law of the Member State transferring the data so provides because of:
> (i) legitimate specific interests of the data subject; or
> (ii) legitimate prevailing interests, especially important public interests; or

[143] Art. 12(2).
[144] Art. 12(3)(a).
[145] Art. 12(3)(b).
[146] Ibid., Art. 25.
[147] Ibid., Art. 26(1).
[148] 2008/977/JHA, Art. 17(1).
[149] Art. 17(2).
[150] Art. 13(1).

(b) the third State or receiving international body provides safeguards which are deemed adequate by the Member State concerned according to its national law."[151]

Instances in which data mining programmes rely on data located in databases in foreign countries will be rare if they occur at all. However, there is likely to be interest in feeding data obtained from foreign authorities, or in some instances, private parties into local databases that support data mining operations. The OECD Guidelines and the Council of Europe Convention on Automatic Processing allow such transfers but permit states to deny transfer when the receiving party does not provide a comparable level of data protection. With the exception of purely intelligence-related work or emergencies, the EU Framework Decision will likely apply to the international transfer of data for data mining purposes. Thus, states would have to ensure that logs of the data transferred are maintained and that the rights of data subjects to receive information as to whether their personal data has been transferred to another country are observed, except where refusal to provide such information is a necessary and proportionate means of protecting national security, ongoing legal proceedings or criminal investigations, or the rights and interests of the data subject or others. Transfers to non-EU countries would only be permissible under the conditions outlined in Article 13(1), including, in particular, the requirement that the state in which the receiving party is located has comparable data protection law in place. Exceptions would only be permitted to protect the rights of the data subject, where overriding public interest considerations made the transfer necessary, or where the state for which the receiving party is acting provided other safeguards which represented an appropriate substitute for the lack of national data protection law.

3.3.3. Sensitive Data

One of the features that distinguishes the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data from the OECD Guidelines is its creation of "special categories" of data. These are data that reveal "racial origin, political opinions or religious or other beliefs" or concern "health or sexual life" or criminal convictions. According to the Convention, these types of data may not be subjected to automatic processing unless the member state provides "appropriate safeguards" within national law.[152] The EU Data Protection Directive also establishes a number of bases for processing sensitive data—i.e. the special categories of data—without the subject's consent that are not found in the Convention.[153] Also unlike the Convention, the Directive requires that the processing of sensitive data otherwise be prohibited by law.[154] The EU Framework Decision only permits the transfer of sensitive data among police and judicial authorities in different states where it is "strictly necessary."[155]

The issue of handling sensitive data is likely to arise in the context of counter-terrorism data mining since such programmes may make use of sensitive data, such as race or national origin, religious or political beliefs. The state would have to ensure that such data is protected by "appropriate safeguards". This requirement implies that states need to provide a higher level of protection for sensitive data than is the case for other types of

[151] Art. 13(3).
[152] Art. 6.
[153] See 95/46/EC, Art. 8(2).
[154] Art. 8.
[155] Art. 6.

personal data. Sensitive data that is transferred internationally within the context of judicial cooperation can only take place where it constitutes a necessary measure.

3.3.4. Automated Decisions

Another notable feature of the EU Data Protection Directive with relevance for data mining is Article 15, which concerns "automated decisions". Article 15 mandates that member states must provide all persons with the right to be free from any decision that "produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him".[156] However, the Article also permits a broad exception where such automated decision-making "is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests."[157] Yet, should such automated decisions be implemented, Article 13 requires that any data subject whose data is subjected to such decisions be given the right to obtain "knowledge of the logic involved in any automatic processing of data concerning him".

The EU Framework Decision also addresses automated decisions in Article 7. This article provides that automated decisions that have adverse legal effects for the data subject or significantly affects him must have a basis in national law. Additionally, the law must provide safeguards to protect the data subject's legitimate interests.

Data mining represents an automated process and if data mining is used as the sole basis of an administrative action that affects the rights of individuals, aspects of data protection law relating to automated decisions are implicated to the extent applicable. The EU Framework Decision applies to international transfers of data that fall within the realm of law enforcement as opposed to national security intelligence. Thus, where data obtained from foreign authorities forms the basis of an automated decision supported by data mining, the state needs to have appropriate legal provisions in place that explicitly authorize the operation and provide protections to safeguard individual rights. In practice, data mining is generally not the sole basis for administrative decisions, but may provide the point of departure for a series of events that lead up to a decision. For instance, data mining is often used to single out individuals for closer scrutiny and further investigation may lead to a decision with adverse consequences for that individual's rights. Whether such uses of data mining represent the rendering of automated decisions is likely to depend upon the precise facts and circumstances in each case. The decision to single out an individual for greater scrutiny—implicating the right to respect for private life—may in itself represent an automated decision with adverse effects on the rights of individuals.

3.4. Conclusion

Although data protection law may have limited application in the realms of law enforcement and national security, certain aspects of data protection law will apply. In particular, the OECD Guidelines ensure that the basic principles of data protection generally apply to counter-terrorism data mining and the EU Charter provides basic rights which can only be limited to the extent necessary for the protection of national security. Article 7 of the

[156] Art. 15(1).
[157] Art. 15(2)(b).

Council of Europe Convention on Automatic Processing will also apply, requiring that states provide adequate security measures for the protection of personal data. Additionally, the EU Framework Decision applies whenever a programme makes use of personal data that has been transferred from another state. Moreover, as noted above, the ECtHR will enforce aspects of the Convention on Automatic Processing within the context of Article 8 of the ECHR. Thus, data protection law will effectively be imposed under the rubric of the right to respect for private life.

4. Non-Discrimination

4.1. Law

The UDHR, the ICCPR, the ECHR, and the EU Charter of Fundamental Rights all contain provisions guaranteeing the right to equality and non-discrimination on the basis of, among other grounds, race, colour, national origin, religion, and gender. Additionally, at the UN level, the Convention on the Elimination of All Forms Racial Discrimination (CERD) and the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) provide more specific provisions pertaining to racial and gender discrimination, respectively.

4.1.1. Scope

Article 1 of the UDHR declares that all human beings are equal in dignity and rights. Article 2 provides that all persons are entitled to the rights and freedoms laid out in the Declaration "without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." Article 7 guarantees equality before the law, as well as equal protection of the law, for all persons

Similarly, the ICCPR calls on signatories to respect and ensure the Covenant rights for all individuals "without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status" in Article 2 and to guarantee the equal enjoyment of civil and political rights under the Convention for both men and women in Article 3. Article 26, in contrast, guarantees non-discrimination not only in the context of other rights but in general and is thus an "autonomous norm". It guarantees equality before the law and equal protection of the law for all persons and calls for the prohibition of any form of discrimination and equal and effective protection for all persons against such discrimination. In addition to the grounds of distinction explicitly listed in Articles 2 and 26 of the ICCPR, differential treatment on the basis of a wide range of further grounds has been recognized as an interference with the right to non-discrimination, including the grounds of nationality[158] and age.[159] The Covenant prohibits not only direct discrimination but also so-called indirect discrimination. Thus, measures which do not appear discriminatory on their face, but nonetheless result in a disproportionate impact on a particular group or class, represent an interference with the right to be free from discrimination under the ICCPR.[160]

[158] Gueye v. France (196/1985).
[159] Schmitz-de-Jong v. The Netherlands (855/1999).
[160] Althammer v. Austria (998/2001).

The ECHR declares in Article 14 that the "enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status." An additional protocol, Protocol 12, has also been drafted and has been ratified by 18 member states of the Council of Europe.[161] The substantive part of the Protocol consists of two provisions. The first provision is identical to Article 14 with the exception that it applies to "any right set forth by law" as opposed to the "the rights and freedoms set forth in this Convention". The second provision prohibits discrimination against any person at the hands of "any public authority on any ground such as those mentioned in [the first provision]."

Article 14 of the ECHR is a "subordinate" or "parasitic" provision in that it only applies to discrimination that involves the enjoyment of another right or freedom guaranteed by the ECHR.[162] According to the ECtHR, in order to invoke Article 14, an applicant must show that the facts of the case fall "within the ambit" of another substantive Convention right.[163] However, there is no need to show that there has been *a violation* of that Convention right. Due to the inclusion of the "other status" category, the number of grounds of differential treatment which may be found to violate Article 14 is theoretically unlimited.[164]

The ECHR may also prohibit indirect discrimination as suggested by the *DH v. Czech Republic* case.[165] There, the applicants argued that they had been discriminated against as members of the Roma community by being placed in special schools for intellectually less able children where they received an inferior education. Although the local educational policy did not directly discriminate against Roma, it ultimately had a discriminatory result, since a disproportionate number of Roma children were sent to the special schools as compared with non-Roma children.[166] As applicants may find it very difficult to prove that an apparently neutral measure has a disproportionate impact on particular groups, the ECtHR held in *DH* that less strict evidential rules should apply in cases of indirect discrimination: "statistics which appear on critical examination to be reliable and significant" may be sufficient prima facie evidence of indirect discrimination.[167]

The Charter of Fundamental Rights of the European Union prohibits in Article 21(1) discrimination on the basis of "any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation." Article 21(2) prohibits discrimination on the basis of national origin "[w]ithin the scope of application of the Treaty establishing the European Community and of the Treaty on European Union".

4.1.2. Justified Differential Treatment

[161] Council of Europe Treaty Office at http://conventions.coe.int (visited 5 July 2011).
[162] See D. J. Harris, M. O'Boyle, E. P. Bates and C. M. Buckley, *Law of the European Convention on Human Rights*, 2. ed. (Oxford: Oxford Univ. Press, 2009), p. 578; D. Moeckli, 'Equality and Non-discrimination', in D. Moeckli, S. Shah and S. Sivakumaran (eds), International Human Rights Law (Oxford, Oxford University Press, 2010) 189, pp. 194-196.
[163] Rasmussen v. Denmark (1984) 7 EHRR 371, para. 29.
[164] Harris, O'Boyle , p. 584
[165] App. No. 57325/00 (2007).
[166] Ibid., pp. 607–8
[167] Ibid., para. 188.

According to the established jurisprudence of both the HRC and the ECtHR, differential treatment may be justified under the ICCPR and the ECHR if it is based on reasonable and objective criteria.[168] The ECtHR has articulated the criteria for distinguishing between justified and unjustified differential treatment as follows: "[T]he Court, following the principles which may be extracted from the legal practice of a large number of democratic states, holds that the principle of equality of treatment is violated if the distinction has no objective and reasonable justification. The existence of such a justification must be assessed in relation to the aim and effects of the measure under consideration, regard being had to the principles which normally prevail in democratic societies. A difference of treatment in the exercise of a right laid down in the Convention must not only pursue a legitimate aim: Article 14 is likewise violated when it is clearly established that there is no reasonable relationship of proportionality between the means employed and the aim sought to be realised."[169] This test, requiring that any difference in treatment must (1) pursue a legitimate aim and (2) be proportionate, is very similar to the test used to assess the permissibility of limitations of Article 8 of the ECHR, described above.

Certain grounds of distinction are regarded as inherently suspect and therefore require particularly strict scrutiny. The grounds attracting the greatest degree of attention and most likely to be declared unjustified are race, ethnicity, sex, and religion.[170] With regard to ethnicity, for example, the ECtHR has stressed that "no difference in treatment which is based exclusively or to a decisive extent on a person's ethnic origin is capable of being objectively justified in a contemporary democratic society built on the principles of pluralism and respect for different cultures."[171] Similarly, with regard to distinctions based on sex the Court has observed that "very weighty reasons would have to be advanced before a difference in treatment on the ground of sex could be regarded as compatible with the [ECHR]."[172]

4.2. Implications for Data Mining

4.2.1. Whether Data Mining Represents Differential Treatment

As noted in D08.2, some forms of data mining effectively amount to profiling. Although profiling need not include consideration of personal characteristics, some programmes have clearly included or intend to include considerations of sex, age, race, national or ethnic origin, and religion. The German *Rasterfahndung* is one clear example, but also systems that rely on Advance Passenger Information would include criteria such as sex, age, and nationality.[173] The objectives for processing such information may vary from programme to programme. In a best case scenario, an individual's data may simply receive more attention in a back office or national security agency. In other scenarios, a data mining programme may result in a person being subjected to additional screening procedures at an airport. In more extreme scenarios, it may ultimately mean that an individual is prevented from

[168] For ICCPR, see Broeks v. The Netherlands (172/84), ¶ 13; for ECHR, see *Belgian Linguistics Case (No. 2)* (1968) 1 EHRR 252, para. 10 (1968).
[169] Belgian Linguistics Case (No. 2), para. 10
[170] See Moeckli, supra note 162, pp. 202-203.
[171] Timishev v. Russia, App. Nos. 55762/00 and 55974/00, Judgment of 13 December 2005, para 58.
[172] Abdulaziz, Cabales and Balkandali v. UK (1985) 7 EHRR 471, para 78.

[173] Advance Passenger Information includes information contained in a passport. See, e.g., British Airways, "Advance Passenger Information", http://www.britishairways.com/travel/ba6.jsp/imminfo/public/en_gb.

boarding a flight, denied entry to a country, arrested and interrogated, or denied the freedom to pursue economic activities, due to restrictions placed on a bank account.

To the extent that data mining that includes such personal data results in differential treatment for certain groups of persons, it implicates the right to non-discrimination. Since, in addition to potential "second-order violations" of the right to liberty or due process guarantees, all these applications of data mining amount to an interference with the right to privacy, they involve differential treatment that is, in principle, prohibited by the norms guaranteeing non-discrimination referred to above, regardless of whether these are "subordinate norms" (such as Article 14 of the ECHR) or "autonomous norms" (such as Article 26 of the ICCPR).

4.2.2. Whether Differential Treatment May Be Justified

Data mining programmes that involve differential treatment based exclusively or to a decisive extent on one (or several) of the grounds that are treated as inherently suspect (such as race, ethnicity, religion or sex) may never be justified. As far as data mining involves differential treatment based on other grounds or on a combination of a range of factors, it may be justified if it is carried out in pursuit of a legitimate aim and in a manner that is proportionate to that aim.

As stated above, the prevention of terrorism will be recognized as a legitimate aim. The decisive question is therefore whether data mining involving differential treatment is a proportionate means of achieving that objective. Thus, it must be considered, first, whether such counter-terrorism data mining programmes are a suitable and effective means of countering terrorism and, second, what kind of negative effects such programmes may produce.[174]

In D08.2, we found that evidence verifying the relative effectiveness of data mining programmes is generally lacking. We also pointed out that counter-terrorism data mining programmes often involve considerable costs for the respective government agencies (in terms of financial costs, human resources, information overload, following up on false positives etc.) as well as serious negative impacts for those subject to these data mining programmes (in terms of human rights violations). Of course, the proportionality of a given state measure can only be assessed having regard to the specific circumstances of the case at hand. However, what can generally be said is that large-scale data mining programmes that fail to produce any results, involve considerable costs to government agencies and interfere with the human rights of a great number of individuals (such as, for example, the German *Rasterfahndung*) will fail to meet the proportionality test.

5. Best Practices and Guidelines for Human Rights Compatibility

In order to comply with the various requirements established in human rights law presented above, we recommend that states undertake the following measures when implementing data mining programmes for counter-terrorism purposes. We suggest that states will need to establish a legal framework to provide explicit authorization of the programme, notice to

[174] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 29 January 2007, UN Doc A/HRC/4/26, para. 47.

everyone of the use of the programme, and appropriate safeguards for the rights of individuals. Additionally, an institutional framework will be required to provide oversight of the use of the programme and ensure accountability for misuse. Lastly, an implementation framework should be established to ensure ground-level compliance with the law and should include training for agents and officials, the development and implementation of internal procedural rules, and appropriate IT system design and architecture.

5.1. Legal Framework

National law pertaining to the use of data mining programmes for counter-terrorism efforts should provide the following:

a. A description of the offences which the programme will be aimed at addressing or preventing or in the prosecution of which it is intended to assist as well as the precise purpose of the programme

In the event that "terrorism" is explicitly defined in national criminal law, terrorism may be named as an offence for which the programme may be implemented. Additionally, there may be other offences defined in national criminal law that may be related to threats to national security which states may choose to include under the targeted offences of a particular data mining programme. In particular, aviation-related offences such as hijacking or attempts to detonate explosives on aircraft should be named in those programmes aimed at providing airline screening. The use of such programmes, however, may not be permissible to uncover drug trafficking unless the level of intrusion is appropriate for such lesser offences.

b. A description of the classes of persons who fall within the scope of the programme

In addition to the offences which the programme is aimed at addressing, the law should clarify whether the programme will only target suspected (potential) offenders or also their accomplices, associates, etc.

c. A definition of the general scope of operation of the programme

Defining the scope of operation and the context in which a programme will operate reinforces the purpose specification principle and forces decision-makers to contemplate the optimization of effectiveness, while limiting the risk of human rights violations. Additionally, it serves to apprise everyone of the programme's existence and to obtain a general understanding of its function. The law need not describe the operation of the programme in such detail as to allow individuals to circumvent the programme. Nonetheless, it should provide enough information to permit everyone to know under what circumstances their personal data may be subject to processing.

d. Definition of the types of data to be used by the programme

Specifying the type of data to be used by a data mining programme serves to limit the data that is subjected to processing, and thus limits the scope of interference with the right to respect for private life. Additionally, it informs everyone of the nature and extent of interference with their rights that may occur and thus complies with the foreseeability requirement enforced by the ECtHR. Governments should especially avoid the use of types

of data that reflect the race, ethnicity, sex, or religion of data subjects and be hesitant to use data reflecting language, political or other opinion, national or social origin, property, or birth, unless they can demonstrate that the inclusion of such factors genuinely enhances the effectiveness of the data mining programme in question.

e. Definition of the permissible duration of the programme

One distinction in the *Weber* and *Liberty* cases, was the fact that the German statute had placed a default time limit on the use of strategic monitoring, whereas UK law had not defined any such limit. The G10 law in Germany would appear to be aimed at addressing specific, identified threats as opposed to an open, "always on" fishing expedition.[175] The imposition of a time limit would also serve as another limitation on the scope of harm which the use of a programme would incur and provide an opportunity for a post-run review to assess whether further use of the programme was warranted. However, the law should provide that use of the programme should be discontinued immediately if at any time the conditions which justified the initial authorization are no longer present or use of the programme is no longer necessary.

There is, however, a certain conflict in the practice of signals intelligence monitoring and the imposition of time limits since signals intelligence-related monitoring is often used as a means of detecting threats. Thus, states that rely on this form of early warning system may argue that they will be unable to identify specific threats without conducting such persistent surveillance. It is unclear how the ECtHR would react to such arguments. Yet, the same conflict applies to many forms of data mining which are utilized to provide constant background monitoring. The imposition of time limits is not consistent with the purpose of such programmes.

f. The procedure for obtaining a warrant or other form of authorization for the use of the programme, including identification of those parties empowered to grant authorization

The German procedures for authorization of strategic monitoring as outlined in *Weber* met with the ECtHR's approval. One of the features of the German system which distinguished it from that of the UK was the fact that authorization did not rest solely in the hands of one party or agency. A multi-party approval procedure can provide internal checks and balances against abuse of power or neglect in the safeguarding of human rights. Additionally, the German law required that the order authorizing the use of strategic monitoring had to describe and provide reasons justifying the particular nature, scope, and duration of the monitoring. Such a requirement can not only serve in the ex ante assessment of the appropriateness of the measure, as is the case with warrant proceedings, but can also serve to provide a record for ex post review and regular audits for legal compliance.

g. Procedures for data handling, including the period of retention, authorized transfer and sharing of data, and procedures for the destruction of data

The law should provide that personal data be destroyed as soon as they are no longer needed to achieve the purpose of the programme. Procedures should be established in the law that call for periodic review to determine whether any currently stored personal data

[175] Compare also the holding of the *Rasterfahndung* case which declared that such profiling measures could only be conducted to address a concrete terrorist threat.

meet the conditions for destruction.[176] The law should also define destruction in terms of rendering the data completely irretrievable, so that they may not be reconstructed or accessed in any form, using the best technical means and methods available. Standards for the transfer of data both to domestic authorities as well as international authorities should also be defined in law. Transfer to authorities with law enforcement or prosecutorial authority should only occur where necessary to protect a significant legal interest or where there is sufficient basis for the suspicion that the commission of a crime has occurred or is being planned. Data protection principles would require that international transfers should only occur where the recipient state provides an adequate level of data protection.

h. Procedures for notification and remedial procedures

Whenever instances of the use of a data mining programme take place in secret, individuals whose personal data has been subjected to processing may be entitled to notification that their rights have been affected. Once a particular use of data mining has been terminated, affected individuals should be notified of the processing of their data whenever notification would not jeopardize the goals of the programme. Article 13 of the ECHR guarantees the right to an effective remedy before a national authority for any violation of rights provided under the Convention. The provision of remedies for violations involving personal data is also consistent with the data protection principle of accountability. National law should provide some process by which affected individuals may seek redress. Redress may entail the award of monetary compensation in some circumstances. Governments should also develop procedures for eliminating the reoccurrence of false positives that have adverse results for the enjoyment of rights of individuals as well as the correction of incorrect data in underlying databases.

5.2. Institutional Framework

Governments will need to establish an institutional framework for oversight of surveillance powers, including the use of data mining.

a. Procedures for Authorization

Governments may provide that the authorization for the use of data mining originate with a warrant-like proceeding or an executive order. Both the HRC and the ECtHR have shown a preference for reliance on judicial authority. However, the ECtHR found the use of an executive order for strategic monitoring in the *Weber* case to be acceptable in light of the safeguards provided by German law. In either case, the possibility for subsequent judicial review should be provided. Governments that choose to require a warrant proceeding may wish to establish specialized surveillance courts for the exclusive hearing of such matters. Where this is the case, additional measures may need to be taken to ensure that such courts remain independent and critical despite their secret nature.

b. Oversight Authorities

The reliance on oversight mechanisms in which multiple actors with different interests and roles are involved at different stages of the decision-making process can provide a robust system of checks and balances against abuse. Oversight authorities should receive regular reports of the use of data mining and the underlying authorization. Such authorities should

[176] The current version of the G-10 law calls for review every six months. Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, §6(1) (as amended 31 July 2009).

be empowered to examine the justifications given for authorization and question the authorities involved in the decision to provide authorization. Additionally, governments may choose to impose the pre-approval of one or more such oversight bodies as a prerequisite for authorization. Governments should regulate the composition of such bodies or the appointment of persons to such bodies in order to ensure its independence and qualification for its task. Governments should also provide an oversight authority with the power to conduct investigations and discipline malfeasants or wrongdoers. Alternatively or in addition to a review body, such as Europol's Joint Supervisory Body, which conducts regular reviews of data handling practices, governments may choose to assign the national data protection supervisor a role in overseeing data handling procedures.

5.3. Implementation Framework

The implementation framework should be targeted not only at the individuals who will run and operate data mining programmes or have access to the underlying data or data mining results, but also at the system architecture of the information technology resources utilized by such programmes. Additionally, the framework should incorporate a set of internal rules to define procedures for personnel and authorities.

Training
Users of data mining programmes and anyone likely to handle the underlying data or programme results should receive comprehensive training in the legal standards and required procedures falling within the legal framework referenced above. These individuals should also be instructed in the requirements of international and domestic human rights law and data protection standards. Users of data mining programmes and their results should be provided with a substantial understanding of how the programme functions in addition to the required knowledge for its effective use. Instruction in the operation of the programme should include raising awareness of the potential for false positives and other sources of error.

Internal Rules
Internal rules of the relevant government agencies should be developed to provide the following procedures and ensure that agency action is in conformity with legal requirements:

a. Procedures for preserving confidentiality
b. Procedures for disclosure of data mining results and their incorporation into reports
c. Procedures on sharing results and reports (both nationally and internationally)
d. Procedures for the storage, retention, and destruction of data as well as the notification of affected parties

System Architecture
The infrastructure and design of the system performing and supporting data mining should be aimed at minimizing the likelihood of unauthorized access or disclosure. Where feasible, counter-terrorism officials may want to use closed networks that have no access to wider systems or the internet. Systems which may be exposed to the internet or other networks or systems should employ the best possible security to prevent unauthorized access. The system should also be subject to strict access controls. Access should be limited to those individuals who have a real need to use the system for the performance of their duties and

have received the appropriate training in its use and operation as well as those individuals who are charged with maintaining the operation of the system. Access as well as editing, transfer, or deletion of files or data should be logged for quality control and legal compliance purposes. In addition, systems may make use of privacy enhancing technologies such as encryption of the underlying data, anonymization or selected revelation procedures. Selected revelation masks identifying data until the user has demonstrated a need to uncover the identity of a particular individual. Automated processes may also be used to provide auditing. For instance, access logs may themselves be subjected to data mining to identify suspicious instances or patterns of access. Such a use of data mining may also reinforce users' sensitivities to the limits of data mining.